Department of Homeland Security Daily Open Source Infrastructure Report for 22 February 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports a shortage of natural gas forced Xcel Energy to impose controlled outages early Saturday, February 18, in Grand Junction, several mountain communities and metro Denver, Colorado, where below−zero temperatures broke at least one record. (See item 3)
- The Tampa Tribune reports online customers are finding their personal and credit information placed on public Websites used to exchange information on hacking by people waging global jihad. (See item 14)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *February 20, Associated Press (Australia)* — **Mauritania ready to pump first oil.** Mauritania will produce its first oil by the end of this week and hopes to pump 300,000 barrels per day within three to four years, a senior state oil executive said. "The 24th (of February) is the deadline," said Ismail Abdel Vetah of national oil company Societe Mauritanienne des Hydrocarbures. The Chinguetti project, one of five oil discoveries made off Mauritania's shores since 2001, will make Mauritania Africa's newest oil producer and is forecast to yield 75,000 barrels per day. Abdel Vetah said Mauritania should be producing 300,000 barrels per day in

three to four years, once three other fields in the same basin −− Walata, Tevet, and Labeidna −− come on line. "Walata is the most advanced. There are 300 million barrels of recoverable oil," Abdel Vetah said. Initial drilling suggested Tevet held 60 million to 70 million barrels of recoverable oil while Labeidna held around 60 million. A fourth field, Banda, was thought to contain about 50 million barrels, Abdel Vetah said. Mauritania is hoping oil finds under its eastern desert will catapult it into the major league of crude producers. "Currently Mauritania has oil reserves estimated at around 600 million barrels, all offshore," Abdel Vetah said.
Source: http://au.news.yahoo.com/060219/2/xydq.html

2. *February 20, White House* — **President promotes Advanced Energy Initiative.** President Bush is touring the country to promote his Advanced Energy Initiative. The Initiative provides for a 22 percent increase in funding for clean−energy technology research at the Department of Energy. To change how the U.S. powers its homes and offices, the initiative proposes more investment in zero−emission coal−fired plants, revolutionary solar and wind technologies, and clean, safe nuclear energy. The initiative also calls for funding additional research in cutting−edge methods of producing ethanol, not just from corn, but from wood chips, stalks, or switch grass. The President's 2007 Budget includes $250 million for the Global Nuclear Energy Partnership, in which the U.S. will work with nations like France, the United Kingdom, Japan, and Russia that have advanced civilian nuclear energy programs to develop and deploy innovative, advanced reactors and new methods to recycle spent nuclear fuel. Other initiatives include completing a commitment to $2 billion in clean coal technology research funding, and move the resulting innovations into the marketplace. Reducing the cost of solar photovoltaic technologies so that they become cost−competitive by 2015 and expanding access to wind energy through technology, are also emphasized.
President's Advanced Energy Initiative:
http://www.whitehouse.gov/stateoftheunion/2006/energy/index. html
Source: http://www.whitehouse.gov/

3. *February 19, Associated Press* — **Gas shortage cuts power; thousands of customers lose electricity for thirty minutes at a time.** A shortage of natural gas forced Xcel Energy to impose controlled outages early Saturday, February 18, in Grand Junction, several mountain communities and metro Denver, CO, where below−zero temperatures broke at least one record. A natural gas supplier to Xcel had equipment problems, causing a significant loss of electricity generation at the company's natural gas power plants, company spokesperson Tom Henley said. Frozen liquid at the supplier's wellhead slowed the flow of natural gas. The problem was enhanced by increased demand because of the freezing temperatures. Beginning about 8:45 a.m. MST up to 100,000 customers in the Denver area, Grand Junction, Vail, Aspen, and Basalt lost power for about 30 minutes at a time. The outages occurred during a two−hour period. By 1 p.m., Henley said, supply problems were ending. "We don't expect any more, but that situation could change at any time," he said. Between 3,500 and 5,000 customers remained without power Saturday afternoon in mostly isolated incidents, some of which were caused by the frigid weather.
Source: http://www.chieftain.com/national/1140336210/6

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *February 21, Macon Telegraph (GA)* — **Diesel spill closes part of highway in Georgia.** A diesel spill at State University Drive in Fort Valley, GA, closed the road's two southbound lanes for several hours Saturday afternoon, February 18, for cleanup after a tractor−trailer and a car crashed. No one was injured in the wreck, but 150 gallons of diesel fuel spilled onto the roadway after one of the truck's fuel tanks ruptured, Fort Valley Fire Chief Otis Daniel said Monday, February 21. Firefighters used sand to dam up the fuel to prevent it from leaking into the sewer system until a private contractor arrived and was able to clean up the spill, Daniel said. The cleanup took more than seven hours.
Source: http://www.macon.com/mld/telegraph/13921302.htm

5. *February 20, Pawtucket Times (NH)* — **Toxic scare in Rhode Island prompts road closure.** For nearly six hours on Sunday, February 19, a portion of Massasoit Avenue in East Providence, NH, was blocked off to traffic due to a chemical contamination scare at the FujiFilm Company. East Providence fire officials said Sunday night that a broken sprinkler at FujiFilm Electronic Materials U.S.A, Inc. set off the scare at approximately 4 p.m. EST. Because the sprinkler system spilled water into a room that held various chemicals, the fire department was forced to treat the scene as a possible contamination site in case the chemicals reacted with the water. For the next five−and−a−half hours, the East Providence Fire Department worked with the Providence Fire Department's Hazardous Materials Team to figure out exactly what they had on their hands. During that time, Massasoit Avenue was blocked off from Dexter Road to approximately one block past the FujiFilm building at 200 Massasoit Ave. At approximately 9:30 p.m. EST, the Hazmat team concluded that the water had not caused a chemical reaction and that there was no contamination. East Providence fire officials also said that no evacuations were necessary.
Source: http://www.zwire.com/site/news.cfm?newsid=16159881&BRD=1713&PAG=461&dept_id=24491&rfi=6

6. *February 19, Quincy Herald−Whig (IL)* — **Farm chemical company blaze prompts evacuation of one near−by residence in Illinois.** The Illinois State Fire Marshal's Office is investigating a Saturday morning, February 18, blaze that destroyed much of the Helena Chemical Co.'s facility at Camp Point, IL. The call on the fire came in at about 4 a.m. CST Saturday, Camp Point Assistant Fire Chief Jim Potts said. Potts said there was some concern about chemicals at the site, and the Quincy Fire Department's hazardous material team was called in. The business provides farm chemicals, fertilizer and seed to area farmers. However, the amount of chemicals on hand was "very minor," said John Simon, director of the Adams County Emergency Management Agency. The residence of Brent and Jennifer Obert, located just across the road from the facility, was evacuated as a precaution. "The outside impact of this incident was actually very, very, very small," Simon said. The business was formerly known as Walker's Crop Service, and only recently was purchased by Helena Chemical Co., based in Tennessee.
Source: http://www.whig.com/285445809674531.php

7. *February 17, Carlisle Sentinel (PA)* — **Twelve taken to hospital after possible chlorine leak in Pennsylvania.** A suspected chlorine leak led to an evacuation at the West Shore Health Club in Hampden Township, PA, Friday morning, February 17, sending a dozen people to the hospital, authorities said. At about 8:30 a.m. EST emergency responders were sent to the

Hampden Township club and shortly after confirmed that an evacuation of the building was under way. A decontamination tent was set up near the club, where authorities said people were being decontaminated with a portable shower. Rick Flynn, chief of Hampden Fire Co., says a cloud of chlorine gas was released as an employee was maintaining the club's pool. He was mixing hydrochloric acid in a six−gallon bucket when it reacted with a small amount of residual chlorine, Flynn says.
Source: http://www.cumberlink.com/articles/2006/02/17/news/news28a.t xt

[Return to top]

Defense Industrial Base Sector

8. *February 21, Aviation Week* — **Supplemental requests aircraft replacement.** The White House Thursday, February 16, submitted its expected supplemental request to Congress, which among dozens of provisions would provide $389.9 million to fund the replacement of U.S. Air Force MC−130H aircraft, Predator drones, C−17 spares and various other items. A total of $65.3 billion of the new $72.4 billion request is for the Department of Defense, while $2.9 billion is for intelligence community and classified programs supporting global antiterrorist operations. The request includes $8.3 billion to refurbish or replace equipment that is worn out or damaged from operating in harsh conditions in Iraq and Afghanistan, $2 billion for counter−improvised explosive device efforts, and $2.6 billion for adding armor to all convoy trucks and buying armored security vehicles, night−vision equipment and helicopter survivability systems. Besides Air Force aircraft, the supplemental would provide $500 million to fund procurement of Army AH−64 aircraft destroyed in Iraq and Afghanistan, and $33.2 million for modifications to sensor equipment on other Army aircraft. For the Navy, the supplemental would fund $271.3 million worth of UH−1 Navigation Thermal Imaging Systems, F/A−18 listening pods, AV−8B upgrades, aircraft fuel tanks, aircraft air foils and AV−8B kit installations for the Joint Direct Attack Munitions.
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily _story.jsp?id=news/SUPP02216.xml

9. *February 21, Agence France−Presse* — **Asian Aerospace show opens in Singapore.** Asian Aerospace, Asia's top air show, opened Tuesday, February 21, to showcase civilian and military equipment from around the globe. More than 900 exhibitors from 43 countries have displays at the event which runs until Sunday, February 26. Attendance is expected to top the 75,000 trade visitors and curious members of the public who visited the last event in 2004, organizer Reed Exhibitions said. U.S. manufacturer Boeing and Europe’s Airbus are the major rivals seeking to show off their latest products to potential buyers at the world’s third−largest air show.
Source: http://www.defensenews.com/story.php?F=1548655&C=asiapac

10. *February 21, Agence France−Presse* — **Experts: High−tech weapons could minimize casualties in urban war.** Fears of high casualty rates from old−fashioned bloody hand−to−hand combat have made military commanders dread urban combat. But high−tech weaponry including precision guided bombs, unmanned vehicles and powerful armored tanks have reduced troops’ exposure to life−threatening situations, military experts said at an Asian security conference Monday, February 20. As cities become more populated and extremist networks seek refuge in urban centers, conventional armed forces worldwide need to evolve

their doctrines and weapons to better fight a new kind of enemy, the experts said. ”The urban fight was one that many years ago was considered a place that you did not want to fight,” said Lieutenant General Thomas Metz, the former senior ground tactical commander of U.S.−led coalition forces in Iraq from January 2004 to February 2005. While the advice of the ancient Chinese military strategist Sun Tzu against attacking cities was true in his time, it has become unavoidable in modern warfare, Metz said. Urban warfare necessitates a new set of doctrines that involve mobilizing specialized forces, new tactics and a complex mix of psychological warfare and information operations.
Source: http://www.defensenews.com/story.php?F=1548669&C=asiapac

[Return to top]

Banking and Finance Sector

11. *February 21, Channel Register (UK)* — **Active cookies aim to thwart cyber crooks.** A new technique to protect users against more sophisticated forms of cybercrime has been developed by Indiana University School of Informatics and affiliated start−up RavenWhite. The "active cookie" can be used as a countermeasure against online scams such as pharming and man−in−the−middle attacks. "There are no reliable commercial tools currently available to protect users from such attacks," said Jakobsson of the IU Center for Applied Cybersecurity Research. "We believe that active cookies can provide such protection." Active cookies are a "piece of cached and sandboxed executable code, such as a JavaScript object, that help authenticate an Internet browser to a server," say the researchers. The technology is a shield against identity theft and cyber attacks that can protect against pharming attacks as well as techniques used to hijack Wi−Fi connections or modify consumer router settings. Limitations include limited persistence and a lack of support for roaming users. "And they don't offer security against strong attacks like active corruption of routers on the client−server path, as holistic cryptographic solutions can." Active cookies may be attractive to financial institutions −− they complement existing techniques for user authentication, are easy to use, and don't have the potential security implications associated with browser plug ins.
Source: http://www.channelregister.co.uk/2006/02/21/active_cookie/

12. *February 20, WJXT 4 (FL)* — **New Internet scam targets online sellers.** Crooks on the Internet have been posing as middlemen, targeting anyone selling a high−priced item online. The scam works like this: A seller wants to use the Internet to sell his car. The seller sets the price at $7,000. The seller will begin to receive offers on the car via e−mail, but one offer stands out. Someone posing as a broker working for a client looking for a car just like yours is willing to pay full price. There's a small problem −− the broker tells the seller, "We've successfully bid on an identical vehicle, but it was $4,000 more and we've already had the bank check drawn up for that, but the deal fell through." According to detective Robert Bogers, the broker will then offer to send the seller a cashier's check for $11,000 −− the one from the deal that fell through. The broker will tell the seller to deposit the check and send him the difference. "Many times the bank will give them immediate credit at which time the seller will wire the money back to the suspects," said Bogers. Two or three days later the bank will notify the seller that the deposited check was bad.
Source: http://news.yahoo.com/s/wjxt/20060220/lo_wjxt/3280313

13. *February 20, Sydney Morning Herald (Australia)* — **Suncorp targeted in latest bank scam.** Suncorp−Metway has become the latest Australian bank to be targeted in a phishing scam by scammers attempting to steal personal banking details from customers. The scammers have already heavily targeted larger banks including The Reserve Bank, Westpac, the National Australia Bank, and Commonwealth Bank but may now shifting their focus to regional operations. The latest phishing attack appears as an official looking bank e−mail bearing the Suncorp−Metway logo which informs recipients that the bank is upgrading software. The message instructs customers to click on a link to confirm their data or risk having their account blocked. "This instruction has been sent to all bank customers and is obligatory to follow," the message reads. The scammers do not specifically target bank customers, but send the message out to thousands of e−mail addresses, hoping a few customers will take the bait. The bank is working with the appropriate agencies to shut down the fake sites. According to other banks targeted by the scam, very few customers have been taken in by the fraudulent e−mails because they tended to land in individual e−mail inboxes several times, raising suspicion. The scam perpetrators rapidly change the source and content of their messages to evade detection.
Source: http://www.smh.com.au/news/breaking/suncorp−targeted−in−latest−bank−scam/2006/02/20/1140283988114.html

14. *February 20, Tampa Tribune (FL)* — **Online stores are caught in Jihad Web.** Online customers are finding their personal and credit information placed on public Websites, such as 3asfh.net, that has been used to exchange information on hacking by people waging global jihad. The 2002 explosion that killed more than 200 people at a nightclub in Bali, Indonesia, was financed through credit card fraud. Alan Paller of the SANS Institute said that in a book Imam Samudra −− the perpetrator −− wrote in jail, he "exhorts followers to 'learn to hack.'" The 2003 Information Operations Roadmap, a recently declassified, 74−page Department of Defense report, outlines methods for government agencies to deal with hacking attempts. "Because of the porous nature of security in commerce and finance, and the prevalence of anonymity, it is very easy to siphon and steal funds," said Tom Kellerman, formerly of the World Bank. Kellerman says $400 billion in losses around the world last year resulted from cybercrime, nine out of 10 businesses were affected, and identity theft hit 19.3 million people in the U.S −− a good chunk of which is by jihadi hackers, said Kellerman. Cybercrime on the Internet is "almost like a giant arms bazaar," said Kellerman, where users can download weapons to hack into financial institutions.
Source: http://news.tbo.com/news/metro/MGB47AQ4WJE.html

15. *February 19, Consumer Affairs* — **Verification phishing scam hits Indiana.** Scammers passing themselves off as the "Nationwide Verification Office" have popped up in Indiana this month. Indiana Attorney General Steve Bell says the scam that has targeted mostly seniors in other states has been reported recently all across the Hoosier state. "Callers representing themselves as from Nationwide Verification Office are calling Hoosiers and selling them a story that their bank accounts have been compromised and they need to verify their routing numbers and other personal information," Carter said. Similar schemes have been reported recently in Alabama, Illinois, Michigan, Ohio, Texas, and Wisconsin. In some instances, consumers have been told their banking account information has been posted on the Internet and they need to verify the account number so that the information doesn't "get into the wrong hands." Illinois residents were asked for their account information so that it can be deleted from a so−called "federal banking system." Consumers are asked to verify their bank account

number, or to read it and the bank routing numbers found at the bottom of their checks.
Source: http://www.consumeraffairs.com/news04/2006/02/scam_verificat ion.html

16. *February 17, CNET News* — **New Trojans plunder bank accounts.** Cybercriminals are surfing into online banks with you to steal your money. Password−stealing Trojan horses used to be all the rage. But in response to the increased adoption of stronger authentication, cybercriminals are changing their tactics, according to Alex Shipp of MessageLabs. "We have recently seen a move away from stealing user name and passwords," Shipp said at the RSA Conference 2006. The new "bank−stealing Trojans" wait until the victim has actually logged in to their bank. "It then just transfers the money out...All of the authentication, little keys you have to have in your hand, biometrical things, it doesn't matter. The bad guy just waits until you're there and then takes the money out," Shipp said. This new type of Trojan is on the rise and is currently number three on the list of most common threats, according to Shipp. The bank−stealing Trojans are programmed to work with specific online banking Websites, Shipp said. The malicious software typically arrives in an e−mail with an apparently innocent Web link, for example, to an online greeting card. Clicking on it will download an executable that installs itself into a browser and then waits until a bank site is accessed.
Source: http://news.com.com/New+Trojans+plunder+bank+accounts/2100−7 349_3−6041173.html?tag=cd.top

[Return to top]

Transportation and Border Security Sector

17. *February 21, NorthJersey.com* — **PATH to go "smart card" route.** The Port Authority of New York and New Jersey plans to roll out its $73 million "smart card" system that's expected to make traveling easier for more than 210,000 daily riders on the PATH trains (Port Authority Trans−Hudson). On Monday, February 20, the Port Authority demonstrated how the card, which contains a computer chip, will eventually replace the magnetic−strip technology at the turnstiles. Similar to E−ZPass, the turnstiles now have sensors that read the card −− no direct contact is necessary −− and deduct money from a prepaid account. The cards can be read through clothing and can work as much as six times faster than MetroCards or QuickCards. The Port Authority hopes to attract people who won't ride the PATH because they're fed up with finding change for a fare. The Port Authority also has upgraded its ticket machines to allow riders to add single or multiple fares to their smart card accounts. Eventually, the cards could be linked to a credit card and replenished automatically when balances run low. The Port Authority hopes to eventually expand the system to link to NJ Transit, the Metropolitan Transit Authority, the Long Island Rail Road, and Metro North.
Source: http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnF lZUVFeXkzJmZnYmVsN2Y3dnFlZUVFeXk2ODgzOTQ0JnlyaXJ5N2Y3MTdmN3Z xZWVFRXl5Mg==

18. *February 21, Union−Tribune (CA)* — **Border tunnelers could face 20 years.** Surprisingly, it's not illegal to tunnel into the United States. There are other crimes associated with border tunnels, such as it is illegal to enter the country someplace other than an official border crossing, or to import drugs. And it's illegal to help others do these things. California Senator Dianne Feinstein said she plans to introduce legislation that would set a maximum 20−year

sentence for building or financing a tunnel into the U.S. Landowners who let others build or use such a tunnel would face up to 10 years in prison. And smugglers using a tunnel to move aliens, terrorists, weapons, drugs or other contraband would see their sentences doubled. Eight tunnels between San Diego and Tijuana have been discovered this year, according to Feinstein's office. That's part of the 40 tunnels her office counted since the 2001 terrorist attacks, all but one of them between the U.S.−Mexico border, according to her office. The other one was between British Columbia and Washington. Agents said few people are actually caught, and often the people digging the tunnel don't know who they're working for.
Source: http://www.signonsandiego.com/news/mexico/tijuana/20060221−9999−1m21tunnel.html

19. *February 21, KOMO TV (WA)* — **Debate over arming Canadian border guards.** Canadian patrol agents left their posts twice in the last month because they feared that armed men trying to flee U.S. authorities were headed toward the border. On January 24, there was a shootout at the Peace Arch border crossing as Whatcom County, WA, deputies chased down two California murder suspects and shot one of them. Both were captured on the U.S. side, but some of the Canadian border guards left their posts in case trouble came their way. In both cases, the border was shut down for hours, leaving travelers snarled in the lapse of security coverage. The union representing Canada's agents says the reason they have never carried weapons is an "image thing." They want to portray Canada as peaceful and having a gun strapped to your side doesn't do that. But guards want to provide protection like their armed U.S. counterparts, and stop the inconveniences to travelers trying to head in and out of the two countries. Newly elected Prime Minister Steven Harper arming guards and says he will also look at revamping how many guards are at each post. Often, there is only one guard manning the crossing. The U.S. has at least two per post.
Source: http://www.komotv.com/news/story_m.asp?ID=41955

20. *February 21, Kentucky Post* — **Airport to create a security fast lane.** Air travelers willing to pay more and to provide additional personal information will get speedier trips through security at Cincinnati/Northern Kentucky International Airport located in Hebron, KY, beginning in June. The airport will seek bids on March 3 for a vendor to begin a Registered Traveler program that will pre−screen participants and allow them to pass through their own security line with less scrutiny than other travelers. The airport plans to have the service running by June 20, said Nancy Conrad of the airport staff. The Federal Aviation Administration (FAA) has tested Registered Traveler programs run by several private companies at airports in Orlando, Minneapolis, Houston, Los Angeles, Washington DC, and Boston. Those tests were completed in September, and the FAA is ready to allow all major airports to begin the service.
Source: http://news.kypost.com/apps/pbcs.dll/article?AID=/20060221/NEWS02/602210387/1014

21. *February 21, Department of Transportation* — **Washington Dulles gets $200 million pledge.** Washington Dulles International Airport got a $200 million pledge from the federal government to help build a fourth runway on Tuesday, February 21, when Department of Transportation Secretary Norman Y. Mineta signed a letter of intent to provide funding over the next eleven years for the project. Once the runway and associated taxiways are completed in 2008, it will allow the airport to handle up to 50 percent more flights per hour during the right conditions, Mineta said. He added that the new runway will make it easier for aircraft to land

during bad weather conditions. And, he said the project also would help reduce flight delays nationwide. The new runway is needed because Dulles is one of the fastest growing airports in the country, Secretary Mineta said. Noting that traffic at the airport has grown from twelve million passengers a year in 1996 to over twenty−seven million in 2005, the airport is now among the nation's busiest. Mineta said that the airport has been working over the years to keep pace with its growing passenger load, by expanding its main terminal, adding a new air traffic control tower, and new concourses and building new parking facilities, among other projects. Mineta's remarks: http://www.dot.gov/affairs/minetasp022106.htm.
Source: http://www.dot.gov/affairs/dot2706.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

22. *February 21, Stop Soybean Rust Now News* — **Soybean rust found on kudzu in two Alabama counties.** Alabama officials reported finding soybean rust on kudzu in Baldwin and Mobile counties February 15 while scouting for new and/or old growth and soybean rust in 40 kudzu patches there recently. The two counties border Mobile Bay in far southwest Alabama, making Mobile County the western−most soybean rust find in 2006. Added to the first find of the year in Montgomery County, there are now three positive counties in Alabama. The U.S. total of counties where soybean rust has been confirmed this year is 16, although Georgia just turned Thomas and Grady counties back to "green" for no rust after removing/destroying the plants/leaves that were found to be infected with soybean rust on January 30 and February 10.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=689

23. *February 21, Associated Press* — **Yellowstone again closes bison capture facility.** Authorities at Yellowstone National Park have again closed the corral−like capture facility near the park's northern border, where more than 900 wandering bison have been held this winter. The Stephen's Creek facility was closed in late January, then reopened earlier this month to capture a group of bison that has crossed onto private lands. It was open for eight days before closing again, Yellowstone officials said. Authorities on January 11 began capturing bison that ventured too far into Montana for the first time in two years. Park officials say 939 bison were captured at the Stephen's Creek facility this winter. Of those, 849 were sent to slaughter without being tested for brucellosis. Concerns about the potential spread of the disease brucellosis from migrating bison to cattle in Montana lie at the heart of the state−federal management plan that allows for the hazing and capture of bison that stray. Many of the park's bison have brucellosis, as do some elk in the region. The disease can cause cows to abort.
Source: http://www.casperstartribune.net/articles/2006/02/21/news/wyoming/8dc908d748645f0d8725711a007ec7bd.txt

24.

February 21, Xinhua (China) — **Brazil confirms new foot−and−mouth disease outbreaks.** Another six cases of foot−and−mouth disease (FMD) have been confirmed among livestock raised in Brazil's Parana state near the borders with Argentina and Paraguay, said Minister of Agriculture Gabriel Alvez Maciel on Monday, February 20. The minister said that the ministry had quarantined the affected farms, and informed the Panamerican Animal Health Organization of the cases that have been located in the municipalities of Bela Vista do Paraiso, Grandes Rios, Maringa, and Loanda. "The outbreaks have hit farms which had already been placed under quarantine by the state's veterinary service. Nine farms in Parana were identified as suspicious in November 2005," he said. FMD has been detected in seven of the nine farms, the first of which was announced on December 5. A total of 4,500 heads of cattle raised on the seven affected farms have been ordered by the ministry to be slaughtered, he added. Foot−and−mouth was first detected in October and November 2005 in the state of Mato Grosso do Sul. Authorities are now investigating the links between outbreaks in Mato Grosso do Sul and Parana.
FMD information: http://www.oie.int/eng/maladies/fiches/A_A010.HTM
Source: http://news.xinhuanet.com/english/2006−02/21/content_4206724 .htm

[Return to top]

Food Sector

25. *February 21, Associated Press* — **Japan seeks assurances for U.S. beef.** Japan will resume imports of U.S. beef only if Washington can convince Tokyo that it will implement effective safeguards against mad cow disease, a top Japanese official said Tuesday, February 21. Chief Cabinet Secretary Shinzo Abe said the government was still examining a U.S. Department of Agriculture report on the faulty veal shipment that prompted Japan to close its markets to American beef last month. Japan's agriculture minister said on Monday, February 20, that the report was insufficient and raised a lot of questions, and Prime Minister Junichiro Koizumi said a quick resumption of imports was unlikely. "If, after all that, the U.S. can convince us that preventive measures will be firmly taken from the perspective of food safety and security, then we will resume the imports at that point," Abe told reporters. Japan closed its doors to American beef last month after the discovery of banned backbones in a shipment of U.S. veal, a violation of the pact that reopened Japan's market to the meat in December 2005. Japan eased a two−year−old ban on U.S. beef in December.
Source: http://www.forbes.com/entrepreneurs/feeds/ap/2006/02/21/ap25 39949.html

26. *February 17, U.S. Food and Drug Administration* — **Pinto beans recalled.** La Preferida, Inc. announced Friday, February 17, the voluntary recall of a limited number of its brand−name 15−ounce cans of whole pinto beans as a precautionary measure after a consumer in De Kalb, IL, reported finding a bird's head in a 15 oz. can of the product. La Preferida is working closely with federal, state and local health agencies to investigate the incident. Testing is expected to take place next week to determine how and when the object got into the can. No injury or illness has occurred as a result of the incident. The company has not received any similar reports. The product was canned on behalf of La Preferida by New Meridian Inc. of Eaton, IN. As an initial precaution after receiving the call from the consumer, La Preferida immediately removed all 15 oz. pinto bean cans from the store where the can was purchased.
Source: http://www.fda.gov/oc/po/firmrecalls/lapreferida02_06.html

[Return to top]

Water Sector

27. *February 21, Associated Press* — **St. Cloud issues water alert after bacteria tests.** Residents of St. Cloud and St. Augusta, MN, were asked to continue boiling their water on Tuesday, February 21, after weekend tests found possible contamination of E. coli bacteria. The city put out the alert Monday, February 20, after tests collected over the weekend returned positive E. coli bacteria samples in the water, said Utilities Director Ken Robinson. The St. Cloud School District closed schools on Tuesday. Mayor Dave Kleis said the city was working with retailers to make sure there was plenty of water on their shelves. If tests come back positive for bacteria Tuesday, he said the retailers would work with the city to get water to residents. E. coli can make people sick, especially those with weakened immune systems like children and the elderly. It can cause diarrhea, cramps, nausea, headaches or other symptoms.
Source: http://www.twincities.com/mld/twincities/news/breaking_news/ 13920367.htm

[Return to top]

Public Health Sector

28. *February 21, Associated Press* — **Bird flu confirmed in swans in Hungary.** Test results Tuesday, February 21, confirmed that three dead swans found in Hungary were infected with the H5N1 strain of bird flu, while Malaysia began killing birds after reporting its first case of the disease in more than a year. The three dead swans, found earlier this month near the village of Nagybaracska, about 100 miles south of Budapest, were Hungary's first confirmed cases of H5N1, government spokesperson Andras Batiz said. Hong Kong's government, meanwhile, said a dead magpie found near an urban flower market was infected with the H5N1 strain, and health workers in western India expanded a massive slaughter of chickens. More than half a million birds have been killed in India's Navapur district since the virus was found in samples from some of the 30,000 dead chickens. The government plans to kill a total of 700,000 birds within a 1.5−mile radius of the outbreak in Maharashtra state. Malaysia began culling birds and launched house−to−house inspections for sick people in a central district where 40 chickens last week died from the virus, Health Minister Chua Soi Lek told reporters. The affected villages are just outside Kuala Lumpur, Malaysia's largest city.
Source: http://abcnews.go.com/Health/wireStory?id=1643615

29. *February 21, Reuters* — **Fake drugs thrive on Internet.** Criminals are using the Internet to sell increasing quantities of counterfeit medicines, including fake versions of bird flu drug Tamiflu, a senior United Nations health expert said on Tuesday, February 21. Antibiotics, anti−malarials and pain killers were susceptible to fraud because of the huge demand, while Tamiflu, made by Swiss firm Roche, had also entered the market amid rising avian flu fears. "Yes, there have been cases reported in counterfeit Tamiflu," said Howard Zucker, the World Health Organization's (WHO) assistant director general for health technology and pharmaceuticals. The WHO has estimated as many as 10 percent of drugs on the world market are mislabeled or fake, with the phoney medicines sometimes causing illness and even death in

consumers. Speaking to reporters after a high−level meeting in Rome, Italy, where pharmarceutical industry and health experts agreed to set up a task force to fight the counterfeit drug trade, Zucker said better oversight of online drug sales was essential. At the meeting, the WHO said it would help set up an international expert group to raise awareness about fake drugs and to improve cooperation between governments, industry groups and international agencies on the issue.
Source: http://today.reuters.com/news/newsArticle.aspx?type=healthNews&storyID=2006−02−21T171237Z_01_L2146807_RTRUKOC_0_US−UN−CONTERFEIT.xml

30. *February 21, PLoS Medicine* — **Pandemic influenza: Risk of multiple introductions.** Influenza A (H5N1) viruses have reached high prevalence in both domesticated and wild birds in several parts of Asia; the virus has spread over an area ranging from Romania to Indonesia. Over 160 human cases, about half of them fatal, have occurred, from Indonesia to Turkey. These trends suggest an increasing risk that the virus may acquire the ability to transmit efficiently from human to human, equipping it to cause a pandemic. Multiple measures are required to prevent such a pandemic and, if these fail, to detect it, check its spread, and mitigate its effects. Attention has recently focused on the possibility of containing a pandemic in its earliest phases at its source. First, the strain must be only moderately transmissible, with a basic reproductive number of 1.8 or less −− in other words, containment is likely to work only if each individual infected with the pandemic strain infects an average of 1.8 or fewer individuals. Containment would require that further conditions also be met: the emerging pandemic is detected within the first 20 cases or seven to 21 days; antivirals are delivered efficiently to around 90 percent of clinical cases within two days of symptom onset; the strain remains susceptible to oseltamivir; and adequate antiviral supplies are available.
Source: http://medicine.plosjournals.org/perlserv/?request=get−document&doi=10%2E1371%2Fjournal%2Epmed%2E0030135

31. *February 20, University of Illinois at Chicago* — **Using cell phones to teach pandemic flu preparedness.** A team from the University of Illinois at Chicago (UIC) has developed the first interactive tool using mobile phones to educate the public about pandemic flu. The free, interactive media −− called Mobile PanFlu Prep −− will be demonstrated at the Local, State and Federal Public Health Preparedness Summit February 22 to 24 in Washington, DC. Public launch is March 1. "It seems so logical, but this is the first time that cell phones have been used to communicate valuable public health information for disaster preparedness," said Colleen Monahan, director of the Center for the Advancement of Distance Education at the UIC School of Public Health. Mobile PanFlu Prep can be downloaded to a cell phone as one would download an interactive game. A series of menu items and audio provide the user with information on flu symptoms, advice on avoiding the flu, and a checklist to prepare for pandemic flu.
Source: http://tigger.uic.edu/htbin/cgiwrap/bin/newsbureau/cgi−bin/index.cgi?from=Releases&to=Release&id=1369&frommain=1

32. *February 17, Pune Newsline (India)* — **Preliminary probe shows chikungunya virus in India.** The preliminary investigations into a mysterious fever that wreaked havoc in at least five districts of Andhra Pradesh, India, in January has pointed towards mosquito−transmitted virus as the cause behind it. This chikungunya virus was found to be behind the mysterious fever by a

team of scientists from the National Institute of Virology. The team that visited the districts and collected the samples are yet to finalise their report, but prima facie investigations have all pointed towards the chikungunya virus. Chikungunya virus is highly−infective and disabling. The name comes from Swahili and means "that which bends up" giving a reference to the positions that victims take to relieve the joint pain.
Chikungunya information: http://www.phac−aspc.gc.ca/msds−ftss/msds172e.html
Source: http://cities.expressindia.com/fullstory.php?newsid=170348

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

33. *February 20, Associated Press* — **Texas task force recommends state oversight of evacuations.** The Texas governor should be in charge of ordering hurricane evacuations and ensuring gas and other supplies are available to avoid a repeat of the chaos that plagued Texans fleeing Hurricane Rita, a task force recommended Monday, February 20. "The process could have been smoother," Governor Rick Perry said while announcing the findings of the task force, which held a series of hearings around the state. "This report will improve planning and coordination, which will result in more effective hurricane response when lives hang in the balance and every second counts." The task force, which gathered data and testimony in six cities, made 21 recommendations in five areas: command, control and communication; evacuation of people with special needs; fuel availability; flow of traffic; and public awareness. The task force recommended development of contra−flow plans for major evacuation routes and placement of gas, comfort and medical stations. The group also called for a statewide database of people with special needs; the requirement that all nursing homes and health care facilities have an evacuation plan; and a requirement for school districts to make buses and buildings available to evacuees. Medical supplies also must be available along evacuation routes, the group urged.
Source: http://www.dallasnews.com/sharedcontent/APStories/stories/D8 FT2TRGD.html

34. *February 20, New Orleans City Business (LA)* — **FEMA: First responders will not face homeless future.** As the post−Katrina March 1 pullout of cruise ships housing first responders nears in New Orleans, officials are trying to prevent a housing crisis they fear could result in mass resignations of first responders. Emergency officials said they will hold the Federal Emergency Management Agency’s (FEMA) “feet to the fire” to provide a housing solution by March 1 for at least 400 first responders living on cruise ships at the Port of New Orleans. Katrina resulted in nearly 80 percent of officers losing their homes, according to a recently completed police foundation report. The report said 671 police officers are living on a cruise ship at the Port of New Orleans. Bob Stellingworth, president and CEO of the New Orleans Police Foundation, said FEMA has assured him there are enough 250−square−foot trailers to provide housing for officers when the ships depart. Officials with the police foundation are

concerned a lack of housing could cause the city, which had a recruiting problem before Katrina, to lose officers to higher paying police agencies in other states where their families have been living since the storm.
Source: http://www.neworleanscitybusiness.com/viewStory.cfm?recID=14 761

35. *February 19, Catoosa County News (GA)* — **Georgia to conduct severe weather drill.** Georgia Governor Sonny Perdue has proclaimed the week of February 19−25 as Severe Weather Awareness Week in Georgia. The main event of the annual weeklong awareness campaign is the Statewide Severe Weather Drill, scheduled for the morning of Wednesday, February 22. The National Weather Service (NWS) will initiate the drill.
Source: http://news.mywebpal.com/news_tool_v2.cfm?show=localnews&pnpID=724&NewsID=697978&CategoryID=3418&on=0

[Return to top]

Information Technology and Telecommunications Sector

36. *February 20, Hackers Center* — **Xerox ESS/ Network Controller and MicroServer vulnerability.** Some vulnerabilities have been reported in Xerox WorkCenter Pro and Xerox WorkCenter, which can be exploited by malicious people to bypass certain security restrictions, conduct cross site scripting attacks, or cause a denial−of−service (DoS). Analysis: Unspecified errors in the authentication process can be exploited to bypass the user authentication and gain unauthorized access. An unspecified error within the processing of Postscript requests can be exploited to cause a DoS via a specially crafted request. Unspecified input passed to certain Webpages is not properly sanitized before being returned to users. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site. Unspecified errors can be exploited to reduce the effectiveness of certain security features. The vulnerabilities affect the following products: WorkCenter 232, 238, 245, 255, 265, and 275; WorkCenter Pro 232, 238, 245, 255, 265, and 275.
Solution: Install System Software Version 14.027.24.015 or 13.027.24.015 (the software versions can be obtained by contacting Xerox customer support).
Source: http://www.hackerscenter.com/archive/view.asp?id=22904

37. *February 20, Channel Register (UK)* — **Spammers adopt stealth tactics.** Botnet controllers are switching to stealth tactics in a bid to avoid detection. Instead of mass mail−outs of spam and malicious code, they are adopting slower distribution tactics in a bid to avoid appearing on corporate security radars. UK−based Web security firm BlackSpider Technologies reports that one huge botnet, responsible for issuing 50 million identical spam e−mails per day, compromises at least 150,000 distinct IP addresses. The use of a large number of machines −− each sending out an average of 330 e−mails a day or around 40 per hour during the course of a working day −− is a change from prior botnets when only a handful of compromised e−mail servers would have been used to do the same job. It's well known that packages such as Send−safe.com are used by spammers to control the distribution of junk mail broadband−connected PCs infected by viruses such as SoBig, but BlackSpider's figures on the mail−out rate from compromised machines add a fresh perspective to the problem. BlackSpider Technologies CTO James Kay said this low mail−out rate means users of compromised machines will not notice anything unusual with their net connection. Because they don't notice

anything amiss, the spambot remains undetected.
Source: http://www.channelregister.co.uk/2006/02/20/stealth_spam/

38. *February 17, Tech Web* — **Gartner: Turn off file sharing in Google Desktop.** Tech research firm Gartner Inc. is recommending that enterprises turn off the file−sharing feature in Google Inc.'s desktop software. In a research posting on its site, Gartner said businesses allowing employees to use Google Desktop 3 Beta, which was released February 9, should start using the enterprise version of the software immediately. In addition, it said businesses should disable the Search Across Computers feature. The feature enables people to share files in their computers. Google does this by storing index copies of the files on its server for up to 30 days. The information is encrypted, and computer users decide which files they want to share. The problem with the feature, according to Gartner, is that employees are not always reliable in identifying documents that should not be shared. Such files could include those with regulatory or security restrictions, the researcher said.
Gartner's report: http://www.gartner.com/DisplayDocument?doc_cd=137896
Source: http://www.informationweek.com/news/showArticle.jhtml?articl eID=180204161

39. *February 17, Federal Computer Week* — **DHS official lays out cyber security responsibilities.** The Department of Homeland Security (DHS) wants its technology procurements to meet recognized standards for security and privacy, a senior DHS official said Thursday, February 16. DHS is working with industry and standards bodies to create procurement requirements that meet those standards, said Jonathan Frankel, director of law enforcement and information−sharing policy in DHS' Office of Policy Planning and International Affairs. Once the standards are in place, the procurement policies will ensure that the government only buys from vendors that meet them, Frankel said at the RSA Conference 2006. Speaking for DHS, Frankel said the department's role is establishing a national strategy and providing an overarching vision of cyber security. DHS is improving its situational awareness of cyber attacks through the U.S. Computer Emergency Readiness Team, he said. The department is also working to manage cyber attack risks through the National Infrastructure Protection Plan.
Source: http://www.fcw.com/article92362−02−17−06−Web

40. *February 17, Washington Technology* — **IG: DHS intel systems lack information security controls.** The Department of Homeland Security cannot yet guarantee that its top−secret intelligence systems are out of reach from hackers, according to a new report from the department's inspector general, Richard Skinner. Based on a review of the department's classified intelligence IT systems conducted from May to September 2005, the IG expressed major concern with the management structure overseeing its intelligence systems as they relate to inventory, certification and accreditation, incident detection and response, and information security training and awareness. DHS officials agreed with the recommendations and have begun taking action to address the issues, the report said.
Declassified summary of the IG report:
http://www.dhs.gov/interweb/assetlibrary/OIG_06−13−Dec05.pdf
Source: http://www.washingtontechnology.com/news/1_1/homeland/28025−1.html

41. *February 17, National Journal's Technology Daily* — **Government wants court hearing on BlackBerry usage.** A court adjudicating a patent spat over the BlackBerry communications

device needs to hold a hearing on the technical details of exempting government users from a potential blackout, the Bush administration said Thursday, February 16. The Justice Department filing is the latest salvo in the ongoing saga over whether Judge James Spencer will order the BlackBerry maker Research in Motion to stop distributing and supporting its ubiquitous communications device in the United States. Under federal law, government users are exempt from injunctions in patent−infringement cases and instead can pay royalties. But the government is worried about the effectiveness of any technical solutions implemented to shield government BlackBerry users and its thousands of contractors from an injunction. To exempt users from a service blackout, government officials and contractors first must be identified. As outlined in the government's brief, there appears to be several methods of doing so, but the process of collecting the information involves significant legwork.
Source: http://www.govexec.com/story_page.cfm?articleid=33430&dcn=to daysnews

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of publicly available exploit code for a buffer overflow vulnerability in Windows Media Player plug−in for browsers other than Internet Explorer (IE).

The buffer overflow may be triggered if a user accesses a specially crafted HTML document. Successful exploitation may allow a remote attacker to execute arbitrary code with the privileges of the user.

More information can be found in the following US−CERT Vulnerability Note:

VU#692060 − Microsoft Windows Media Player plug−in buffer overflow
http://www.kb.cert.org/vuls/id/692060

US−CERT urges users and administrators to implement the following recommendations:

Apply appropriate updates and review the workarounds listed in the Microsoft Security Bulletin MS06−006 to mitigate this vulnerability.
http://www.microsoft.com/technet/security/Bulletin/MS06−006. mspx

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 80 (www), 6881 (bittorrent), 25 (smtp), 6346 (gnutella−svc), 445 (microsoft−ds), 15266 (−−−), 3800 (−−−), 54000 (−−−), 9710 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer